Hardening The HumanOS

Executive Summary

Computers store, process and transfer data that is valuable to your organization. As a result, they have been the primary target for cyber attackers. Years ago, exploiting computers was easy, as most operating systems had very little (if any) security. To help address this problem, numerous technical papers were released on how to secure, or harden, operating systems such as Solaris, Linux and Windows. These documents helped create a culture of how to create and maintain secure operating systems, making today's computers far more secure.

People, just like computers, store, process and transfer information that is valuable to your organization. In many ways, people are nothing more than another operating system, the HumanOS. However, very little if anything has been done to secure this operating system; the HumanOS is far behind in terms of security when compared to most other operating systems. As a result, cyber attackers have shifted their focus away from targeting computers to targeting people. This document addresses the human factor by explaining how, just like any other operating system, you can harden the HumanOS.

To secure the HumanOS, you have to first understand its vulnerabilities. Just like any other operating system, people have vulnerabilities that can be exploited. However, instead of vulnerabilities in code, such as buffer overflows or SQl injection, the HumanOS has insecure behaviors. People already know how to read email, use mobile devices, create passwords or post on social networking sites. What they do not know is how to perform these daily actions securely. To secure the HumanOS, your goal is to make them aware of these risks and ultimately change their behaviors. To accomplish this, your organization needs an effective security awareness program designed from the ground up to change behavior.

Misconfigurations / Misconceptions

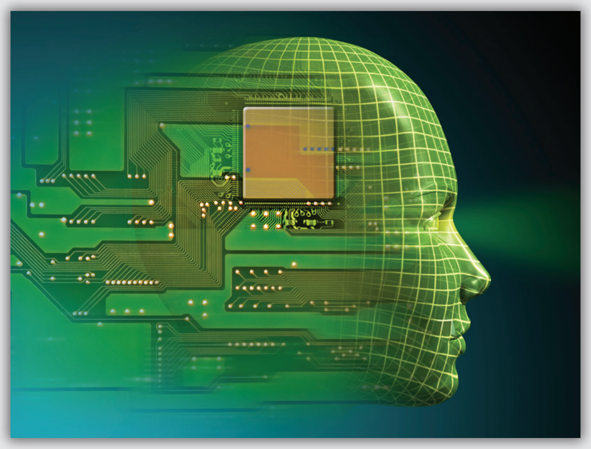
There are several common misconceptions concerning security awareness programs:

1. **Awareness never worked in the past, why should it work now?** The reason most awareness programs have failed to change behaviors is because they were never designed to change behaviors. Most awareness programs were designed only for compliance, keeping auditors happy. This has resulted in programs consisting of nothing more than an annual PowerPoint presentation or a quarterly newsletter. If you patched your computers once a year would you consider them secure? Of course not. Humans are no different. To change human behaviors and secure the HumanOS, you need an active and engaging security awareness program designed from the ground up to do just that. This is what the new generation of security awareness programs are focused on: changing behavior through education on a regular basis.

2. **Someone will always fall victim; as such, awareness is a failure.** A common concern is that no matter how much you train people, someone will always fall victim. As a result, people assume awareness must be a failure. This approach makes no sense. Security is all about reducing risk; we all know and understand

you cannot eliminate it. Security awareness is nothing more than another security control designed to reduce risk just like firewalls, anti-virus or IDS sensors. What is exciting about security awareness is that so little has been done to date to secure people. As such, we have the potential to reduce a tremendous amount of risk to organizations.

3. **Prevention is the only goal.** When people think of awareness training they tend to think only of prevention, the Human Firewall. Prevention is important, but why not go further and also focus on detection and reporting? Create the Human Sensor: teach people, including IT staff and help desk, the most common indicators of compromise and how to detect and report incidents. Remember, we just discussed that security awareness can dramatically reduce human risk, but we cannot eliminate it. What if the small percentage of people who do fall victim realize that something is wrong and immediately report it? This still effectively mitigates the attack. In addition, by creating a Human Sensor network, you improve your organization's overall detection and response capabilities, creating a more resilient network.



Humans, just like computers; store, process and transfer information. People are nothing more than another operating system, the HumanOS. However to date we have done little if anything to secure this operating system, as a result humans are the weakest link in any organization.

Similarities with Other Operating Systems

There are several similarities between hardening the HumanOS and hardening any other OS.

1. **Frequent Updating:** Most operating systems require continuous updating to remain secure. Some operating systems even have a monthly patching cycle where they are updated at a minimum once a month. The HumanOS is no different; it requires continuous, active updating at a minimum once a month.

2. **Changing Risks:** Over time, new programs, code or functionality are added to most operating systems. This means the steps you take to secure them today will evolve and change. Securing the HumanOS is no different. Threat, technologies and business requirements are always changing. You need to ensure that you are, at a minimum, updating your awareness program once a year to address changing human risks.

Differences with Other Operating Systems

The HumanOS also has some unique differences from other standard operating systems.

1. **Emotions:** Unlike other operating systems, the HumanOS has feelings. To change behaviors, you must engage people; you must create a program where people want to learn. One of the key ways to engage is to focus on how people personally benefit from security awareness training. The vast majority of risks people face at work are the very same online risks they face at home, such as email, passwords, mobile devices and social networking. By focusing on how people personally benefit from the training, they are far more likely to listen, learn and change behaviors. In addition, people will now exhibit the same secure behaviors at both home and at work; there is no need to 'change' behaviors when they go to the office. Security becomes part of their DNA.

2. **Misconceptions:** People have a number of misconceptions on security that you may have to address. For example, people often feel that they are not a target because their information or systems have no value and, as such, they do not need to be worried about security. Another common misconception is that people feel they have no role in security. They feel that since organizations implement security technologies, such as firewalls and anti-virus, they do not have to worry about secure behaviors. They do not realize their actions have a direct impact on the security of the organization.

3. **Non-Standardization:** One of the things that makes securing the HumanOS so challenging is that every organization is very different. While most operating system deployments are very similar across most organizations, the industry, structure and culture of your organization is very different from others. As such, your awareness program may be very different from other organizations.

Getting Started

The key to securing the human element is changing their behaviors. To accomplish that, you need a high-impact, engaging security awareness program that focuses on mitigating your top human risks. We can't tell you what those human risks are or how to create your awareness program, as every organization is very different. But we can tell you the key questions to ask. By answering these questions you will help build the foundation for your awareness program:

1. **WHO:** Just as you need to identify which operating systems you will be securing (many organizations support multiple types) you need to identify which people or which roles you will be securing. Will you be providing basic education for all your employees and staff, or will you require additional, specialized training for roles such as senior executives, developers or IT staff? Remember, just because someone is technical does not mean they are secure. In fact, those in technical positions often require additional training, as their privileged access exposes your organization to greater risk.

2. **WHAT:** Once you identify who you are targeting, you need to identify what you will train them on and what behaviors you want to change. For this, you need to identify what your greatest human risks are and which behaviors mitigate those risks. Ultimately, you want to focus on the fewest risks possible. The HumanOS is not good at retaining new information. The fewer risks you address, the easier it is for you to reinforce those key points and the more likely people will remember them and change behavior.

3. **HOW:** Once you identify who you will target in your training and what you will teach them, you need to determine how you will communicate. Communication plays a key role in how successful you are in engaging people. In many ways, security awareness is a product you are attempting to sell, and people in your organization are the customer. The ultimate sign of an engaging awareness program is when employees start asking how their family or friends can take it. You may want to involve marketing or communications from your organization to help with how you communicate your awareness program.

Examples of Changing Behavior

A key part to an effective awareness program is identifying which human behaviors pose the greatest risks to your organization, then establishing an engaging training program that changes those behaviors. Here are several examples of the most common human risks and how they can be mitigated:

1. **Phishing:** One of the most common human risks most organizations face is ‘phishability,’ or people falling victim to email-based phishing attacks. The problem is one of behavior; people are clicking on links or opening attachments with little awareness about the impact of their actions. People need to be trained on how cyber attackers are actively using email to attack them, then teach people the ways to identify common indicators of a phishing email. Once people understand these indicators, they need to be trained on whether they should simply delete such email attacks or report them. One of the most effective ways you can test and reinforce these secure behaviors is not just through standard awareness training, but through actual phishing assessments.

2. **Losing Devices:** Keep in mind that human risks are not just based on malicious attacks. Many incidents are the result of accidental loss or disclosure. For example, if an employee loses a laptop, the data on that laptop may be at risk. The behavior we want to change is to ensure that people know data must be stored on only authorized, secured laptops that have encryption. Data disclosure is when staff accidently share or distribute content to the wrong people (or the public), such as copying the wrong person on an email (auto-complete email features). In this case, we want to change people’s behavior so they always double check to whom their emails are going to when sensitive information is included.

3. **Passwords:** Passwords are one of the most challenging topics to communicate, and one of the most difficult behaviors to change. People not only create weak passwords that are simple to crack or guess, but they use them in insecure manners, such as reusing the same password for multiple accounts or sharing their password with co-workers. As a result, we have two behaviors we want to focus on. The first is ensuring people create strong passwords, perhaps even passphrases. The second is teaching people how to use their passwords securely; to ensure separate passwords for separate accounts and eliminating password reuse. One of the key steps to changing behaviors is not only teaching why they need to change them, but providing the resources and tools they need. For example, if people are using the same password for multiple accounts, they most likely cannot remember many passwords. As such, you may want to consider providing people with a password management tool and teaching them how to use it.

To help you build your security awareness program and harden the HumanOS, including all the different planning steps, documents and checklists involved, we recommend starting with the Security Awareness Roadmap at http://www.securingthehuman.org/resources/planning.

Community Project

This paper was developed by the community for the community. To learn more about this paper or other community projects concerning security awareness, contact **community@securingthehuman.org**. The following people were involved in developing this paper:

Mark Merkow	-	PayPal
Tonia Dudley	-	Honeywell
David M. Vaughn	-	HP Enterprise Services
Vivian Gernand	-	Corning
Tracey Pintell Quade	-	Defense Industry
Robert Maughan	-	Atos Consulting
John Pescatore	-	The SANS Institute
Antonio Merola	-	Poste Italiane